UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/061,415	02/01/2002	Davide Libenzi	002.0259.01	9282

28875 7590 11/09/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/061,415	LIBENZI ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,13-25,28-38,40-47 and 49-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,13-25,28-38,40-47 and 49-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/1/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 8/30/2005.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 8/30/2005 have been fully considered but they are not persuasive. Applicant argues primarily that:

i. Maher did not disclose "passive" monitoring.

ii. Maher did not disclose "datagrams" but instead disclosed "packets".

iii. Maher did not disclose "receiving copies" of datagrams.

iv. Maher did not disclose reassembling into network protocol packets.

v. Maher did not disclose processing based on the transport layer protocol.

vi. Maher did not disclose decoding the reassembled segment prior to scanning.

vii. Maher did not disclose terminating the packet stream if the segment is not infected.

viii. Maher did not disclose all of "logging an infection; generating a warning; spoofing a valid datagram; and acquiescing to the infection.

Regarding applicants' argument i., that Maher did not disclose "passive" monitoring, the examiner has considered the argument and does not find the argument persuasive. The claim requires that only the "network interface" be passive. As clearly disclosed by Maher in Col. 5 Lines 42-57, the fast path data bus receives the framed and formatted data from the physical interface 102, which meets the requirement of the network interface of the claim language

"receiving incoming datagrams structured in compliance with a network protocol layer". Therefore, the examiner does not find the argument persuasive.

Regarding applicants' argument ii. that Maher did not disclose "datagrams" but instead disclosed "packets", the examiner does not find the argument persuasive. Maher disclosed packets throughout the specification (i.e. Col. 5 Lines 63-65) and only disclosed IP type data (See Col. 7 Paragraph 3). As such, Maher disclosed IP packets and because IP packets contain destination address information, they fall within the scope of a "datagram" (See Microsoft Computer Dictionary Fifth Edition Page 143). Therefore the examiner does not find the argument persuasive.

Regarding applicants' argument iii. that Maher did not disclose Maher did not disclose "receiving copies" of datagrams, the examiner does not find the argument persuasive. Maher disclosed receiving data that was taken from the physical ports, framed, and formatted in Col. 5 Lines 42-57. This constitutes "copied datagrams" as the data was "copied" from the data present at the physical ports. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument iv. that Maher did not disclose reassembling into network protocol packets, the examiner does not find the argument persuasive. Maher disclosed assembling ATM cells (data link layer datagrams) into complete data packets, which constitute network protocol packets, in Col. 6 Lines 4-7). Furthermore, the complete packets were stored in the packet storage memory for processing (See Maher Col. 6 Lines 12-14). Therefore, the examiner does not find the argument persuasive.

Regarding applicants' argument v. that Maher did not disclose processing based on the transport layer protocol, the examiner does not find the argument persuasive. Maher disclosed

queuing the packets based on the application type of the packet (i.e. email, VoIP, etc.) in Col. 7 Paragraph 3). The application type is application layer data which could not have been accessed until transport layer processing had been performed. Therefore, it was inherent that Maher performed transport layer processing in order to access the application layer data. Therefore, the examiner does not find the argument persuasive.

Regarding applicants' argument vi. that Maher did not disclose decoding the reassembled segment prior to scanning, the examiner does not find the argument persuasive. Maher in Col. 9 Lines 29-32 disclosed decoding the data to be scanned by removing the white space from the data. Furthermore, it was inherent that the packets were decoded in order to access the payload for scanning. Therefore the examiner does not find the argument persuasive.

Regarding applicants' argument vii. that Maher did not disclose terminating the packet stream if the segment is not infected, the examiner does not find the argument persuasive. Maher disclosed that once the scanning engine had determined that the was no match, the scanning was complete and no further data was required for that flow (See Maher Col. 9 Line 58 – Col. 10 Line 30). As such the examiner does not find the argument persuasive.

Regarding applicants' argument viii. that Maher did not disclose all of "logging an infection; generating a warning; spoofing a valid datagram; and acquiescing to the infection, the examiner does not find the argument persuasive. The claim language does not require all of the listed limitations, but instead only requires "at least one of" them. The sighted section falls within the scope of "spoofing". As such, the examiner does not find the argument persuasive.

Therefore, the examiner has maintained the prior art rejections presented below.

All objections and rejections not presented below have been withdrawn.

Claims 1-10, 13-25, 28-38, 40-47, and 49-55 have been examined.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 32 and 41 recite that "each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram". However, there is no support for this limitation in the specification as filed. See the rejection of claims 32-38, 40-47, and 49-54 under 35 USC 112 1st paragraph below.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 53-54 recite "a plurality of protocol-specific scanning sub-modules, each protocol specific scanning sub-module designated for scanning network protocol packets of a particular protocol". However, there is no support for this limitation in the specification as filed. See the rejection of claims 53-54 under 35 USC 112 1st paragraph below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 32-38, 40-47, and 49-54 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which

was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 32 and 41 recite that "each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram". Although there is support for multiple sub-modules in the scanner, there is no support for a plurality of separate modules which each process each datagram. As such, the ordinary person skilled in the art would not be able to determine whether the applicants were in possession of the claimed invention at the time of filing. Therefore, claims 32 and 41 are rejected for failing to meet the written description requirement of 35 USC 112 1st paragraph. Claims 33-38, 40, 42-47, and 49-54 are rejected by virtue of their dependency to claims 32 and 41.

Claims 53-54 recite "a plurality of protocol-specific scanning sub-modules, each protocol specific scanning sub-module designated for scanning network protocol packets of a particular protocol". Although there is support for the protocol-specific scanning sub-modules, there is no support that they actually scan the packets. Instead, the specification provides support that they simply are used to retrieve the packets and provide them to the scanner. As such, the ordinary person skilled in the art would be unable to determine whether the applicants were in possession of the claimed invention at the time of filing. Therefore, claims 53-54 are rejected for failing to meet the written description requirement of 35 USC 112 1st paragraph.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-10, 13-14, 16-25, 28-29, 31 and 55 are rejected under 35 U.S.C. 102(e) as being anticipated by Maher, III et al. (US Patent Number 6,381,242) hereinafter referred to as Maher.

Regarding claim 1, Maher disclosed a system for providing passive screening of transient messages in a distributed computing environment (See Maher Abstract), comprising: a network interface passively monitoring a transient packet stream at a network boundary (See Maher Column 5 lines 46-54 and Col. 7 Lines 13-15) comprising receiving incoming datagrams structured in compliance with a network protocol layer (See Maher Col. 5 Lines 46-54 and Col. 3 Lines 54-67 wherein it was inherent that the packets were compliant with a network layer in order for them to be transmitted through the network); a packet receiver reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer (See Maher Col. 5 Line 60 - Col. 6 Line 7); an antivirus scanner scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents (See Maher Col. 10 Lines 42-46), and a protocol-specific

module processing each reassembled datagram based on the transport layer protocol employed by the reassembled datagram (See Maher Col. 7 Lines 18-30).

Regarding claim 16, Maher disclosed a method for passive screening of transient messages in a distributed computing environment (See Maher Abstract), comprising: passively monitoring a transient packet stream at a network boundary (See Maher Column 5 lines 46-54 and Col. 7 Lines 13-15) comprising receiving incoming datagrams structured in compliance with a network protocol layer (See Maher Col. 5 Lines 46-54 and Col. 3 Lines 54-67 wherein it was inherent that the packets were compliant with a network layer in order for them to be transmitted through the network); reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer (See Maher Col. 5 Line 60 - Col. 6 Line 7); scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents (See Maher Col. 10 Lines 42-46), and processing each reassembled datagram based on the transport layer protocol employed by the reassembled datagram (See Maher Col. 7 Lines 18-30).

Regarding claims 2 and 17, Maher disclosed an incoming queue staging each incoming datagram intermediate to reassembly (See Maher Col. 8 Lines 42-51).

Regarding claims 3 and 18, Maher disclosed a network protocol-specific decoder decoding the reassembled segment prior to scanning (See Maher Col. 5 Line 65 – Col. 6 Line 1).

Regarding claims 4 and 19, Maher disclosed that the antivirus scanner terminates the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware (See Maher Col. 7 Lines 30-33).

Regarding claims 5 and 20, Maher disclosed that the antivirus scanner takes an action if the reassembled segment is infected with at least one of a computer virus and malware (See Maher Col. 10 Lines 42-46).

Regarding claims 6 and 21, Maher disclosed that the action comprises at least one of logging an infection; generating a warning; spoofing a valid datagram in place of the infected datagram (See Maher Col. 10 Lines 42-46); and acquiescing to the infection.

Regarding claims 7 and 22, Maher disclosed a protocol-specific queue staging each reassembled segment with other reassembled segments sharing the same transport protocol layer (See Maher Col. 7 Lines 18-30).

Regarding claims 8 and 23, Maher disclosed an information record storing information dependent on the same transport protocol layer with the staged reassembled segment (See Maher Col. 6 Lines 12-22).

Regarding claims 9 and 24, Maher disclosed a contents record storing the contents with the staged reassembled segment (See Maher Col. 6 Lines 12-19).

Regarding claims 10 and 25, Maher disclosed that the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject (See Maher Col. 6 Lines 20-22).

Regarding claims 13 and 28, Maher disclosed an event correlator analyzing the transient packet stream for events indicative of a network service attack (See Maher Col. 7 Lines 35-50).

Regarding claims 14 and 29, Maher disclosed a data repository maintaining each event (See Maher Col. 7 Lines 40-48).

Regarding claim 55, Maher disclosed that the incoming datagrams include IP datagrams that are reassembled into TCP segments (See Maher Col. 6 Lines 4-7 and Col. 7 Paragraph 3 wherein it was inherent that the PDUs of the email data was processed to TCP segments in order to get the payload of the data for scanning.)

Claim 31 is rejected for the same reasons as claims 16-25, and 28-29 and further because Maher disclosed processors executing the described functions (See Maher Col. 11 lines 34-37).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 32-35, 38, 41-44, 47, and 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher, as evidenced by Stevens (TCP/IP Illustrated Vol. 1).

Regarding claim 32, Maher disclosed a system for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising: a network interface receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied fro a packet stream (See Maher Col. 5 Paragraph 4 Fast Access Bus); a packet receiver reassembling one or more of the incoming datagrams from the incoming packet queue into network protocol packets, each

staged in a reassembled packet queue (See Maher Col. 5 Line 60 - Col. 6 Line 14); an antivirus scanner scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware (See Maher Col. 10 Lines 42-46), and an event correlator evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain (See Maher Col. Col. 7 Lines 35-50), and disclosed determining the type of data the packets contained (See Maher Col. 7 Paragraph 3) as well as scanning the payload of the packets (See Maher Col. 10 Lines 42-46), however Maher failed to disclose how the data type of the packet was ascertained or how the payload was retrieved.

It was well known that in the Internet Protocol there are multiple layers and that each layer contains different modules, such as the TCP module and the UDP module of the transport layer. It was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet. This is evidenced by Richards Pages 6-11.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art of networking and TCP/IP in order to gain access to the data in the packets for scanning and queuing. This would have been obvious because the ordinary person skilled in the art would have been motivated to use what was well known in the art.

Regarding claim 41, Maher disclosed a method for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising: receiving copies of datagrams transiting a boundary of a network domain into an

incoming packet queue, each datagram being copied fro a packet stream (See Maher Col. 5 Paragraph 4 Fast Access Bus); reassembling one or more of the incoming datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue (See Maher Col. 5 Line 60 - Col. 6 Line 14); scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware (See Maher Col. 10 Lines 42-46), and evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain (See Maher Col. Col. 7 Lines 35-50), and disclosed determining the type of data the packets contained (See Maher Col. 7 Paragraph 3) as well as scanning the payload of the packets (See Maher Col. 10 Lines 42-46), however Maher failed to disclose how the data type of the packet was ascertained or how the payload was retrieved.

It was well known that in the Internet Protocol there are multiple layers and that each layer contains different modules, such as the TCP module and the UDP module of the transport layer. It was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet. This is evidenced by Richards Pages 6-11.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art of networking and TCP/IP in order to gain access to the data in the packets for scanning and queuing. This would have been obvious because the ordinary person skilled in the art would have been motivated to use what was well known in the art.

Regarding claims 33 and 42, Maher disclosed a parser parsing each reassembled datagram into network protocol-specific information and packet content (See Maher Col. 5 Line 65 – Col. 6 Line 19).

Regarding claims 34 and 43, Maher disclosed extracting the header information from the packets (See the rejection of claim 33 above), but failed to disclose specifically what information was contained in the headers. It was well known in the art at the time of invention that the headers of HTTP messages contained a source address and port number, a destination address and port number, and a URL, the headers of an FTP message contained the filename and username, and the headers for the SMTP contained the sender identifier, receiver identifier, and subject. As such, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known by extracting the header information from the headers of the packets. This would have been obvious because the ordinary person would have been motivated to extract what was known to be contained in the header.

Regarding claim 35 and 44, Maher disclosed a decoder decoding the packet content prior to performing the operation of scanning (See Maher Col. 5 Line 65 – Col. 6 Line 1 and Col. 2 Lines 9-12).

Regarding claim 38 and 47, Maher disclosed a spoof module sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and the network attack (See Maher Col. 10 Lines 42-46).

Claim 50 is rejected for the same reasons as claims 32-33, 35, 38, 41-42, 44, and 47 and further because Maher disclosed processors executing the described functions (See Maher Col. 11 lines 34-37).

Regarding claim 51, Maher disclosed that the packets comprised general "web surfing" traffic, email traffic, and VoIP traffic (See Maher Col. 7 Paragraph 3), but failed to specifically disclose the specific protocols used for each. It was well known at the time invention that general web surfing traffic utilized HTTP, and that email traffic utilized SMTP (Simple Mail Transport Protocol) and POP3. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art by using the HTTP, SMTP, and POP3 protocols. This would have been obvious because the ordinary person skilled in the art would have been motivated to use the protocols that were standard in the art.

Regarding claim 52, Maher disclosed that only datagrams compliant with IP protocol are reassembled (See Maher entire reference especially the last paragraph of Col. 3, wherein only IP type traffic was disclosed).

Claims 15, 30, 40, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher as applied to claims 1, 16, 32, and 41 above, and further in view of Hailpern et al. (US Patent Number 6,275,937) hereinafter referred to as Hailpern.

Maher disclosed a system for scanning IP network packets for viruses (See the rejection of claim 1 above and Col. 3 Lines 54-67), but failed to disclose that all the incoming messages were SMTP compliant, and therefore TCP compliant.

Hailpern teaches that virus scanning should be set up for each network protocol proxy, including E-mail, in order to scan for viruses (See Hailpern Col. 4 Lines 1-13).

It would have been obvious to the ordinary person skilled in the art to employ the teachings of Hailpern in the virus scanning system of Maher by modifying mail servers to contain the scanning system of Maher. This would have been obvious because the ordinary

person skilled in the art would have been motivated to enable the proxies to be able to scan the types of communications they already process and therefore reduce network traffic and delay. Further, SMTP mail servers were well known in the art at the time of invention, and it would have been obvious to utilize the scanning system of Maher in an SMTP mail server. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect SMTP mail servers from viruses.

Claims 36-37 and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher as applied to claims 32 and 41 above, and further in view of Bates et al. (US Patent Number 6,785,732) hereinafter referred to as Bates.

Maher disclosed detecting viruses in network packets (See the rejection of claim 38 above), but failed to disclose logging the detection or generating a warning.

Bates teaches that upon detecting a virus, the detection should be logged and a warning should be generated (See Bates Col. 12 Lines 41-48 and Col. 10 Lines 2-8).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Bates in the packet scanning system of Maher by logging virus detections and generating warnings in the event of virus detection. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the server to analyze the virus activity and to alert the sender of the virus of the virus.

Claims 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher as applied to claim 32 above, and further in view of Epstein et al. (US Patent Number 6,684,329) hereinafter referred to as Epstein.

Maher disclosed scanning packets for viruses (See Maher Col. 6 Line 59 – Col. 7 Line 6), but failed to disclose sub-modules which each scan one of HTTP, FTP, SMTP, and NNTP packets.

Epstein teaches that in a firewall which scans for viruses, proxy sub-modules should be provided in the firewall for each of HTTP, FTP, SMTP, and NNTP protocol packets (See Epstein Col. 1 Lines 27-53 and Col. 3 Lines 8-21).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Epstein in the virus scanning of Maher by providing protocol specific proxy servers in the firewall to scan each of HTTP, SMTP, FTP, and NNTP packets. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the network administrator with greater control over the traffic which traversed the content processor.

Conclusion

Claims 1-10, 13-25, 28-38, 40-47, and 49-55 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
11/3/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100